# Online Security Tips/Alight Protection Program™

**Nokia needs you to do your part!**
Take steps to reduce the risk of fraud and loss to your Nokia pension and/or retirement benefit(s). The Department of Labor's Employee Benefits Security Administration recommends following these basic rules:

**Set Up and Routinely Monitor Your Online Benefit Account(s)**

- Maintaining online access to your pension/retirement benefit account(s) allows you to protect and manage your plan benefit(s).
- Regularly checking your benefit account(s) reduces the risk of fraudulent account access.
- Failing to register for access to your benefit account(s) online may enable cybercriminals to assume your online identity.

**Use Strong and Unique Passwords**

- Don't use dictionary words.
- Use letters (both upper and lower case), numbers, and special characters.
- Don't use letters and numbers in sequence (no "abc," "567," etc.).
- Use 14 or more characters.
- It is recommended you don't write passwords down. But, if you must, keep in a secure place.
- Consider using a secure password manager to help create and track passwords.
- Change passwords every 120 days or immediately if you become aware of a security breach.
- Don't share, reuse, or repeat passwords.

**Keep Personal Contact Information Current**

- Update your contact information (phone, email, address, etc.) to ensure you are receiving timely information regarding your pension/retirement account(s).
- Add a mobile phone number to your account so that you can reset your password immediately by receiving and using a One-Time-Code. See more information below.

**Use Multifactor Authentication**

- Multi-Factor Authentication (also called two-factor authentication) requires a second credential to verify your identity (e.g., by entering a code sent to you in real-time by text message or email).
- If you log on to the YBR website using an unregistered device, you will need to enter your username and password and a second credential to validate your identity. The NBRC uses temporary access codes sent to you via your mobile or landline phone or security questions that you have previously set up in YBR. To set up security questions, select the profile icon then select "My Profile", "Log On Information", and "Security Questions". If you cannot recall your password, you have only two options to obtain a password reset and access your account:
    1. One-Time-Code – Allows immediate access. Requires you to have a mobile phone on file with the NBRC that accepts text messages.
    2. A password reset mailed to your address of record on file with the NBRC sent via US Postal Mail. Allow 7-10 business days for mailing.

**Be Wary of--or, Better Still, Avoid--Free Wi-Fi**

- Free Wi-Fi networks, such as the public Wi-Fi available at airports, hotels, or coffee shops, pose security risks that may give criminals access to your personal information.
- A better option is to use your cellphone or home network.

**Watch out for Phishing Attacks**

- Phishing attacks are designed to trick you into sharing your passwords, account numbers, and sensitive information, and gain access to your accounts.
- Don't click on unknown or suspicious links! A phishing message might look like it comes from a trusted organization, to lure you to click on a dangerous link or share confidential information.
- Here are some common warning signs of a phishing attack:
  - Messages that you didn't expect or that comes from a person or service you don't know.
  - Spelling errors or poor grammar.
  - Mismatched links--a seemingly legitimate link sends you to an unexpected address (often, but not always, you can spot this by hovering your mouse over the link without clicking on it, so that your browser displays the actual destination).
  - Shortened or odd links or addresses.
  - An email request for your account number or personal information (legitimate providers should never send you emails or texts asking for your password, account number, personal information, or answers to security questions.
  - Offers that seem too good to be true, express great urgency, or are aggressive and scary.
  - Strange or mismatched sender addresses.
  - Anything else that makes you feel uneasy.

**Use Antivirus Software and Keep Apps and Software Current**

- Have trustworthy antivirus software installed and updated on your computers and mobile devices to protect them from viruses and malware
- Keep all your software on your computers and mobile devices up to date with the latest patches and upgrades. (Many vendors offer automatic updates.)

**Consider Taking Additional Steps Outlined in the Alight Protection Program™**

- The Alight Protection Program ™[1] (the "Program") is available to you at no cost and will reimburse you for losses due to unauthorized activity in your plan account(s) when certain requirements are met.
- Information about the Program, including Program requirements, frequently asked questions ("FAQs"), and instructions on making security updates to your plan record is available in the Security Center section of the Your Benefits Resources (YBR)™[2] website at https://digital.alight.com/nokia, 24 hours a day, seven days a week.

If you suspect that you have been the victim of identity theft or a cybersecurity incident, contact the Nokia Benefits Resource Center (NBRC) at 1-888-232-4111 (or at 1-212-444-0994 if calling from outside of the U.S., Puerto Rico, or Canada). The NBRC is managed by Alight Solutions, LLC., the record keeper for Nokia of America Corporation pension and retirement benefit plans.

View and manage your pension and retirement benefit account(s) online via the Your Benefits Resources™ website at https://digital.alight.com/nokia.

[1] The Alight Protection Program is a trademark of Alight Solutions LLC.
[2] Your Benefits Resources is a trademark of Alight Solutions LLC.